CODING THE REAL LOCUS OF $X_0^+(N)$

CARLOS CASTAÑO-BERNARD

Abstract. Let $X_0^+(N)$ be the Atkin-Lehner quotient of the modular curve $X_0(N)$ associated to the Fricke involution w_N. Assume $N \geq 5$ prime and endow the real locus $X_0^+(N)(\mathbb{R})$ with the real topology. In this paper we revisit a special case of a result due to Ogg on the connected components of $X_0^+(N)(\mathbb{R})$. Then we obtain a formula for the homology class of each connected component of $X_0^+(N)(\mathbb{R})$ in terms of Manin symbols.

Contents

1. Introduction

Fix a positive integer N and let $X_0(N)$ be the moduli space of (ordered) pairs (E, E') of generalised elliptic curves E and E' linked by a cyclic isogeny $\varphi\colon E \longrightarrow E'$ of degree N. The set of real points $X_0(N)(\mathbb{R})$ endowed with the real topology was studied independently by Ogg [14] and Akbas [1]. They described the connected components of $X_0(N)(\mathbb{R})$ and found a simple formula for the number ν_N of connected components of $X_0(N)(\mathbb{R})$. (Cf. Singerman and Akbas [2, p. 6].) Ogg [14] also described the set of real points $(S/w)(\mathbb{R})$ of quotients S/w, where S is the standard Shimura curve associated with an Eichler order of an indefinite quaternion algebra over the rational numbers

$\mathbb{Q}$, and w is an Atkin-Lehner involution. His general result applies in particular to the Atkin-Lehner quotient $X_0^+(N)$ of the curve $X_0(N)$ associated to the Fricke involution w_N, and in particular it may be obtained from it the following result.

Theorem 1.1 (Ogg). *Endow the real locus $X_0^+(N)(\mathbb{R})$ with the real topology. Assume $N \geq 5$ prime. The real locus $X_0^+(N)(\mathbb{R})$ has exactly*

$$\kappa_N = \begin{cases} \frac{h(4N)+h(N)}{2}, & \textit{if } N \equiv 1 \pmod 4 \\ \frac{h(4N)+1}{2}, & \textit{otherwise,} \end{cases}$$

connected components, where $h(D)$ is the number of proper equivalence classes of primitive binary quadratic forms of discriminant D.

In this paper we revisit the above theorem. Our approach is constructive and uses a geometric coding algorithm of level N for indefinite binary quadratic forms. (Cf. Katok [11].) Then we use this coding algorithm to obtain a formula for the homology class of each connected component of $X_0^+(N)(\mathbb{R})$ in terms of Manin symbols [13].

It is hoped that the study of the real points on $X_0^+(N)$ will be of use later on in the study of the rational points of $X_0^+(N)$. (Cf. Shimura [16, p. 1] and Ogg [14, p. 278].) In fact Theorem 1.1 answers question (3) raised by Shimura [16, p. 1], for the case of the quotient curve $X_0^+(N)$ with $N > 5$ prime. So it seems natural to raise here a special case of question (4) of Shimura [16, p. 1]:

how many of the components of $X_0^+(N)(\mathbb{R})$ are homologically independent?

The formula that converts (modulo homology) each connected component of $X_0^+(N)(\mathbb{R})$ into Manin symbols may be used as a computational tool to answer the above question numerically for moderately large prime levels N. (In a forthcoming paper we shall discuss such numerical evidence.)

1.1. **Organisation of the material.** In Section 2 we attach to each indefinite form Q, with non-square discriminant D a smooth path in the Riemann surface $X_0(N)(\mathbb{C})$. Section 3 contains the proof of Theorem 1.1. The proof uses results of Section 2 and basic properties of the negative Pell equation known to Legendre [12], the law of quadratic reciprocity, and the principal genus theorem of Gauß [9]. In Subsection 4.1 we briefly review a geometric coding theory from the author's Ph. D. thesis. Subsection 4.2 contains the formula that expresses the homology class of each connected component of the real locus $X_0^+(N)(\mathbb{R})$ in terms of M-symbols.

1.2. **Acknowledgements.** We would like to thank David Singerman for his helpful comments. The author is indebted to his wife, Concepción Vargas-Chávez and to his brother, Ricardo Castaño-Bernard for their constant support and encouragement.

2. Regular path attached to an indefinite form

2.1. **The level one case.** Let $[A,B,C](X,Y) = AX^2+BXY+CY^2$ denote a binary quadratic forms with real coefficients A, B, and C. Note that for any real numbers α,β,γ and δ we have

$$[A,B,C](\alpha X+\beta Y,\gamma X+\delta Y) = \begin{pmatrix} \alpha^2 & \alpha\gamma & \gamma^2 \\ 2\alpha\beta & \alpha\delta+\beta\gamma & 2\gamma\delta \\ \beta^2 & \beta\delta & \delta^2 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix}.$$

Let $M = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ and define

$$\sigma_M = \det(M) \begin{pmatrix} \alpha^2 & \alpha\gamma & \gamma^2 \\ 2\alpha\beta & \alpha\delta+\beta\gamma & 2\gamma\delta \\ \beta^2 & \beta\delta & \delta^2 \end{pmatrix}^{-1}.$$

Let $\mathcal{Q}$ denote the set of binary quadratic forms. Note that

$$\langle Q,Q'\rangle = BB' - 2(AC'+A'C).$$

makes $\mathcal{Q}$ a quadratic space and $M \mapsto \sigma_M$ defines a group homomorphism

$$\sigma : \mathrm{GL}_2(\mathbb{R}) \longrightarrow O^+(\mathcal{Q})$$

of the general linear group $\mathrm{GL}_2(\mathbb{R})$ into the group of orientation preserving automorphisms $O^+(\mathcal{Q})$ of the ternary quadratic form $|Q|^2 = \langle Q,Q\rangle$ on $\mathcal{Q}$.[1] For each matrix $M \in \mathrm{GL}_2(\mathbb{R})$ and each binary quadratic form $Q \in \mathcal{Q}$ we write $M \circ Q = \sigma_M Q$. The ternary quadratic form $|Q|^2 = \langle Q,Q\rangle$ is called the *discriminant* of the binary quadratic form $Q=[A,B,C]$. We say Q is *definite* (resp. *indefinite*) if $|Q|^2>0$ (resp. $|Q|^2<0$). If Q is *definite* and $A>0$ then we say Q is *positive definite.*

Definition 2.1. Two binary quadratic forms Q_1 and Q_2 are called *equivalent* if there exists $M \in \mathrm{SL}_2(\mathbb{Z})$ such that $M \circ Q_1 = Q_2$.

Let $Q=[A,B,C]$ be a primitive indefinite binary quadratic form. Its *discriminant* is the integer $D = B^2-4AC>0$. Assume that D is non-square so that Pell's equation

$$X^2 - DY^2 = 1 \tag{2.1}$$

has integral solutions. Let $(x,y) \in \mathbb{Z}\times\mathbb{Z}$ be one such solution and consider the automorph of Q defined by

$$M_Q = \begin{pmatrix} x-By & -2Cy \\ 2Ay & x+By \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

[1]In fact the homomorphism σ_M restricted to $\mathrm{SL}_2^{\pm}(\mathbb{R}) = \{m \in \mathrm{GL}_2(\mathbb{R})\colon \det m = \pm 1\}$ is a degree 2 cover of $\mathrm{SL}_2(\mathbb{R})$ known as the spin representation attached to the ternary quadratic form $|Q|^2 = \langle Q,Q\rangle$.

Note that given a base-point $\tau_0 \in \gamma_Q$, the geodesic segment $\{\tau_0, M_Q\tau_0\}$ is a subset of the geodesic

$$\gamma_Q = \left\{ \frac{-B-\sqrt{D}}{2A}, \frac{-B+\sqrt{D}}{2A} \right\}.$$

We shall assume further that $x > 0$ and $y > 0$ so that the eigenvalue $\lambda_Q = x + y\sqrt{D} > 1$ and thus $\{\tau_0, M_Q\tau_0\}$ and γ_Q have the same orientation. So by standard results of hyperbolic geometry as in Beardon's book [3], we may see that the arc-length parametrisation of the geodesic segment $\{\tau_0, M_Q\tau_0\}$ is the restriction of the arc-length parametrisation of the geodesic γ_Q starting at the base point τ_0 to the closed interval $[0, l(Q)] \subset \mathbb{R}$, where $l(Q) = 2\log(\lambda_Q)$ is the hyperbolic length of $\{\tau_0, M_Q\tau_0\}$. Now let

$$g_{Q,\tau_0} \colon\ [0, l(Q)] \longrightarrow X(1).$$

be the map induced in the quotient $X(1) = \mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H}^*$, where as usual the matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{R})$ act on $\mathcal{H}^*$ by fractional linear transformations

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

We shall assume further that the solution (x, y) is minimal subject to the conditions $x > 0$ and $y > 0$, so that M_Q is not a non-trivial power of an element in the modular group $\Gamma(1)$. This means that *essentially* g_{Q,τ_0} traces out its path only once. We call $g_{Q,\tau}$ the *closed geodesic*[2] associated to the form Q and the point $\tau_0 \in \gamma_Q$.

Let X be any differentiable manifold and let T be a positive real number. Recall that a differentiable path $g : [0, T] \longrightarrow X$ is called *regular* if the derivative $g'(t) \neq 0$, for each $t \in [0, T]$.

Lemma 2.2. *Again let Q be an indefinite form and τ a point of γ_Q. The path $g_{Q,\tau} \subset X(1)$ is regular if and only if $\gamma_Q \subset \mathcal{H}$ contains no elliptic elements.*

Proof. It is a well-known classical fact that the complex-analytic structure of the affine modular curve $Y(1) = \Gamma(1)\backslash\mathcal{H}$ is induced by the map $j \colon \mathcal{H} \longrightarrow \mathbb{C}$, where $j(\tau)$ is the elliptic modular function

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \dots,$$

Moreover, given any point $b \in \mathcal{H}$ there is a sufficiently small neighbourhood U (resp. V) of b (resp. $j(b)$) together with an holomorphic identification $\phi \colon U \longrightarrow \mathbb{D}$ (resp. $\psi \colon V \longrightarrow \mathbb{D}$) with the unit disk

$$\mathbb{D} = \{z \in \mathbb{C} \colon |z| < 1\}$$

[2]In the literature the closed geodesic g_{Q,τ_0} is also known as a *prime geodesic*. By the Prime Geodesic Theorem of Sarnak [15] we know that the distribution of the lengths $l(Q)$ is similar to the distribution of prime numbers.

such that the diagram

$$\begin{tikzcd} U \arrow[r, "j"] \arrow[d, "\phi"] & V \arrow[d, "\psi"] \\ \mathbb{D} \arrow[r] & \mathbb{D} \\ z \arrow[r, mapsto] & z^n \end{tikzcd}$$

commutes, where

$$n = \begin{cases} 3, & \textit{if } b \textit{ is an elliptic point of order } 3, \\ 2, & \textit{if } b \textit{ is an elliptic point of order } 2, \\ 1, & \textit{otherwise.} \end{cases}$$

So there is $t_0 \in [0, l(Q)]$ such that $g_{Q,\tau_0}(t_0)$ is an elliptic point then if and only if the derivative $g'_{Q,\tau_0}(t_0) = 0$. The lemma follows. $\square$

For the rest of the subsection suppose g_{Q,τ_0} fails to be regular at a point $t_0 \in [0, T]$, i.e. $g_{Q,\tau_0}(t_0) = \tau_e$, where τ_e is (the image in $X(1)$ of) an elliptic point of order $e = 2$ or 3. Shortly we shall see how, under certain mild conditions, a suitable restriction of the path g_{Q,τ_0} may be extended in a natural way to produce an regular analytic path. But first we need to prove a couple of elementary lemmas on square roots of certain 2 by 2 matrices, and to introduce a further definition. The mentioned regular path is actually constructed in the proof of Theorem 2.6.

Lemma 2.3. *Let Q and M_Q be as above. Also let $\epsilon = x' + y'\sqrt{D} \in \mathcal{O}_D^\times$ (with x' and y' in $\frac{1}{2}\mathbb{Z}$) be a fundamental unit of the real quadratic order $\mathcal{O}_D$ of discriminant D. Assume that ϵ has negative norm $\mathcal{N}(\epsilon) = -1$ and also that $\epsilon > 1$. Then*

$$M_Q^{\frac{1}{2}} = \frac{1}{\sqrt{D}} \begin{pmatrix} Dy' - Bx' & -2Cx' \\ 2Ax' & Dy' + Bx' \end{pmatrix} \in SL_2(K)$$

is a square root of M_Q such that the arc-length parametrisation of the geodesic segment $\{\tau_0, M_Q^{\frac{1}{2}}\tau_0\}$ is the restriction of the arc-length parametrisation of the geodesic segment $\{\tau_0, M_Q\tau_0\}$ to the interval $[0, \frac{1}{2}l(Q)]$.

Proof. Consider the matrix

$$M = \begin{pmatrix} \frac{-B+\sqrt{D}}{2A}c & \frac{-B-\sqrt{D}}{2A}d \\ c & d \end{pmatrix} \in \mathrm{SL}_2(K)$$

where c and d are integers such that $cd = \frac{A}{\sqrt{D}}$. It is plain that the matrix M maps the elements 0 and ∞ as follows:

$$0 \mapsto \frac{-B - \sqrt{D}}{2A},$$
$$\infty \mapsto \frac{-B + \sqrt{D}}{2A}.$$

Now recall that the solution $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ of Equation 2.1 is minimal subject to the conditions $x > 0$ and $y > 0$. In particular the eigenvalue $\lambda_Q = x + y\sqrt{D}$ of M_Q is the generator of the cyclic subgroup

$$\{z \in \mathcal{O}_D^\times : \mathcal{N}(z) = 1 \,and\, z > 1\}.$$

Now consider that the fundamental unit $\epsilon = x' + y'\sqrt{D}$ has negative norm $\mathcal{N}(\epsilon) = -1$. Thus $\epsilon^2 = \lambda_Q$ (since both, $\lambda_Q > 1$ and $\epsilon > 1$). Hence $M \left(\begin{smallmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{smallmatrix} \right) M^{-1} \in \mathrm{SL}_2(K)$ is a square root of M_Q. It is plain that

$$M \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix} M^{-1} = \frac{1}{\sqrt{D}} \begin{pmatrix} Dy' - Bx' & -2Cx' \\ 2Ax' & Dy' + Bx' \end{pmatrix},$$

and the equality in the lemma follows. Now using (once more) that $\epsilon > 1$, the latter part of the lemma follows. □

Lemma 2.4. *The matrix*

$$S^{\frac{1}{2}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

is the square root of $S = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix} \right)$.

Proof. The lemma follows after a straight forward calculation. □

Definition 2.5. Let X be a topological space and let T_1 and T_2 be positive real numbers. Suppose we have paths $f_1 : [0, T_1] \longrightarrow X$ and $f_2 : [0, T_2] \longrightarrow X$ such that $f_1(T_1) = f_2(0)$. The *concatenation* $f_1 * f_2$ of f_1 and f_2 is the path

$$f_1 * f_2 : [0, T_1 + T_2] \longrightarrow X,$$

where

$$(f_1 * f_2)(t) = \begin{cases} f_1(t) & \text{if } 0 \le t < T_1, \\ f_2(t - T_1) & \text{if } T_1 \le t \le T_1 + T_2, \end{cases}$$

for each $t \in [0, T_1 + T_2]$.

Theorem 2.6. *Let Q and τ_0 be as above. Assume that γ_0 contains elliptic point b of degree $e = 2$ not equivalent to τ_0. Further assume that the fundamental unit ϵ of $\mathcal{O}_D$ has norm $\mathcal{N}(\epsilon) = -1$. Then there is a regular analytic path ρ_{Q,τ_0} on $X(1)$ such that, up to a continuous reparametrisation of g_{Q,τ_0}, the restrictions of ρ_{Q,τ_0} and g_{Q,τ_0} to $I = [0, t_0)$ coincide*

$$\rho_{Q,\tau_0} | I = g_{Q,\tau_0} | I,$$

for $t_0 \in \mathbb{R}_{>0}$ sufficiently small.

Proof. Suppose γ_Q contains an elliptic point τ_e of order $e = 3$. By the commutative diagram in the proof of Lemma 2.2 we may see that for a small enough open neighbourhood U of τ_e there is a continuous reparametrisation of the restriction $g_{Q,\tau_0}|V$ of g_{Q,τ_0} to the preimage $V = g_{Q,\tau_0}^{-1} U$, such that $g_{Q,\tau_0}|V$ is both, analytic and regular. Without

loss of generality we may assume $b = \sqrt{-1} \in \mathcal{H}$. The proof splits in two steps as follows.

Step 1. We claim that the path g_{Q,τ_0} may be decomposed as

$$g_{Q,\tau_0} = \{\tau_0, b\}_{\Gamma(1)} * \{b, \tau_0\}_{\Gamma(1)} * \{\tau_0, b'\}_{\Gamma(1)} * \{b', \tau_0\}_{\Gamma(1)}, \tag{2.2}$$

where $X_{\Gamma(1)}$ denote the image of a set $X \subset \mathcal{H}^*$ in $X(1)$, and $b' = M_Q^{-\frac{1}{2}} b$. Now it suffices to prove that b' is an imaginary quadratic number of discriminant $\Delta = -4$. If we consider the positive definite form $P = [1, 0, 1]$, our claim follows if we prove that $P' = M_Q^{-\frac{1}{2}} \circ P$ is integral, primitive, and has discriminant $\Delta = -4$. From Definition 2.1 and Lemma 2.3 we get

$$P' = [1 + 2x^2 - 2Bxy, 8Axy, 1 + 2x^2 + 2Bxy],$$

where $x + y\sqrt{D} \in \mathcal{O}_D^\times$ is a fundamental unit (of negative norm) of the real quadratic order $\mathcal{O}_D$, and D is the discriminant of Q. So x and y both lie in $\frac{1}{2}\mathbb{Z}$. (By a slight abuse of notation we have written x and y instead of x' and y'.) In particular we may see P' is integral. Now suppose P' is not primitive. So $M_Q^{-\frac{1}{2}} \circ P' = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \circ P$ is not primitive, but $P = [1, 0, 1]$ is obviously primitive. We have reached a contradiction. Therefore P' must be primitive. Since it is plain that P' has discriminant $\Delta = -4$, our claim follows. A consequence of our claim is that the path g_{Q,τ_0} not only fails to be regular at the points b and b'; these points are cusps (in the sense of differential geometry) of the path g_{Q,τ_0}.

Step 2. Now we claim that the path ρ_{Q,τ_0} obtained by replacing in the right hand side of Equation 2.2

$$\{b, \tau_0\}_{\Gamma(1)} * \{\tau_0, b'\}_{\Gamma(1)} * \{b', \tau_0\}_{\Gamma(1)}$$

by

$$\{b, b''\}_{\Gamma(1)} * \{b', \tau_0\}_{\Gamma(1)},$$

where $b'' = M^{\frac{1}{2}}_{S^{\frac{a}{2}} \circ Q} b$ and $a = \mathit{sign}(A)$, yields a regular analytic path. Denote ρ_{Q,τ_0} the path thus obtained. Since we assumed that $\tau_0 \neq b$, the length $t_0 = l(\tau_0, b) > 0$. So $p|I = g_{Q,\tau_0}|I$, where $I = [0, t_0)$. Now using the commutative diagram of the proof of Lemma 2.2, and the assumption that b has ramification degree $e = 2$, we may conclude that the path ρ_{Q,τ_0} is regular and analytic at the point b, after a continuous reparametrisation of p. Clearly the same is true for p at b' and the lemma follows. $\square$

Example 2.7. Consider the indefinite form $Q = [1, 4, -1]$ of discriminant $D = 20$, and let τ_0 be the imaginary quadratic number $\tau_0 = \frac{-3+\sqrt{-19}}{2} \in \gamma_Q$. So $b = i$, $b' = i - 4$, and $b'' = i + 1$, as depicted in Figure 2.1.

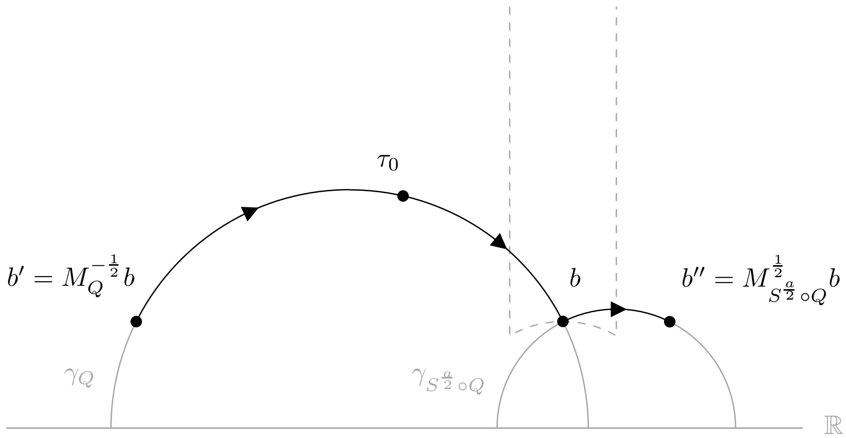

FIGURE 2.1. The path $\{\tau_0, b\} * \{b, b'\} * \{b'', \tau_0\}$.

Remark 2.8. As before suppose that γ_Q contains an elliptic point τ_e of order $e = 2$. Note that the path g_{Q,τ_0} is generically $2 : 1$ onto its image, whereas the path ρ_{Q,τ_0} is generically $1 : 1$ onto its image. This explains the italics in the word "essentially" by the beginning of this subsection, when describing how g_{Q,τ_0} traces out its image.

2.2. **Extension to higher levels.** Note that $\Gamma^0(N) = S^{-1}\Gamma_0(N)S$, where $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. By a slight abuse of notation[3] from now on we write

$$X_0(N) = \Gamma^0(N)\backslash\mathcal{H}^*.$$

As before let $Q = [A, B, C]$ be primitive indefinite form with non-square discriminant $D = B^2 - 4AC$. Now define $M_{N,Q} = M_Q^n$, where

$$M_Q = \begin{pmatrix} u - Bv & -2Cv \\ 2Av & u + Bv \end{pmatrix} \in \Gamma(1),$$

and $(u, v) \in \mathbb{Z}$ is a fundamental solution of the ordinary Pell equation

$$X^2 - DX^2 = 1,$$

and n is the smallest positive integer such that $M_Q^n \in \Gamma_0(N)$. Now pick a base point τ_0 of γ_Q and let g_{N,Q,τ_0} denote the image of the path $\{\tau_0, M_{N,Q}\tau_0\}$ in the modular curve $X_0(N)$. The construction of the regular path in the proof of Theorem 2.6 carries over to $X_0(N)$ as follows. It is well-known that the elliptic points $\tau_e \in \mathcal{H}$ for the action of $\Gamma^0(N)$ in the upper half plane $\mathcal{H}$ are precisely the ones attached to primitive forms $P = [A, B, C]$ with $N \mid C$ and discriminant $\Delta = -3$, if the degree of the point is $e = 3$ and discriminant $\Delta = -4$, if the degree

[3] It is more customary to write $X^0(N) = \Gamma^0(N)\backslash\mathcal{H}^*$. But we want to avoid writing non-standard expressions such as $X_+^0(N)$ (or $X^{0+}(N)$) when considering the Atkin-Lehner quotient defined by the Fricke involution w_N.

of the point is $e = 2$. Assume there is an elliptic point τ_e of degree $e = 2$, e.g. $\tau_e = r + \sqrt{-1} \in \mathcal{H}$ with $r \in \mathbb{Z}$ such that

$$r^2 \equiv -1 \pmod N,$$

and that γ_Q contains such elliptic point τ_e. The matrix $S^{\frac{1}{2}}$ in the said construction is to be replaced by $T^r S^{\frac{1}{2}} T^{-r}$, where and $T = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Again let n be the smallest positive integer such that M_Q^n lies in $\Gamma^0(N)$. Further assume that the fundamental unit ϵ of the real quadratic order $\mathcal{O}_D$ has norm $\mathcal{N}(\epsilon) = -1$. The matrix $M_Q^{\frac{1}{2}}$ is to be replaced by $M_{N,Q}^{\frac{1}{2}} = (M_Q^{\frac{1}{2}})^n$, so that $(M_{N,Q}^{\frac{1}{2}})^2 = M_{N,Q}$. Let ρ_{N,Q,τ_0} be the regular analytic path thus obtained and call it the *regular path of level* N attached to Q. This path is unique up to a regular analytic reparametrisation.

3. Construction of the components

3.1. **On the negative Pell equation.** Let A be any positive integer. It is well-known that the *ordinary* Pell equation

$$X^2 - AY^2 = 1 \tag{3.1}$$

has integral solutions, provided A is not a perfect square. Replacing above "1" by "-1" leads to a completely different situation. In general there seems to be no simple way to decide (e.g. by a congruence condition) whether the *negative* Pell equation

$$X^2 - AY^2 = -1 \tag{3.2}$$

has integral solutions.[4] However, for A prime there is a simple criterion to decide if the (latter) equation is solvable.

Lemma 3.1 (Legendre)**.** *Suppose A is a prime number. Then Equation 3.2 has integral solutions if and only if $A \equiv 1 \pmod 4$.*

Proof. Our proof follows closely (42) and (43) in § VII (p. 64) of Legendre [12]. Suppose (u, v) is the smallest integral solution of Equation 3.1 such that both $u > 0$ and $v > 0$. We can write

$$(u + 1)(u - 1) = Av^2.$$

Since A is prime we have either

$$u + 1 = fg^2A \quad \textit{and} \quad u - 1 = fh^2$$

or else

$$u + 1 = fg^2 \quad \textit{and} \quad u - 1 = fh^2A.$$

So either

$$-\frac{2}{f} = h^2 - Ag^2$$

[4]The study of these Pell equations has a long and outstanding history. (See Weil's book [17].)

or else

$$\frac{2}{f} = g^2 - Ah^2,$$

for suitable integers g and h. The latter two equations imply that either $f = 1$ or $f = 2$. So one of the following possibilities must arise:

$$h^2 - Ag^2 = -1 \tag{1}$$
$$h^2 - Ag^2 = -2 \tag{2}$$
$$g^2 - Ah^2 = 1 \tag{3}$$
$$g^2 - Ah^2 = 2 \tag{4}$$

On the one hand note that (3) contradicts the minimality assumption on (u, v), while on the other, the assumption $A \equiv 1 \pmod 4$ clearly implies neither (2) nor (4) is possible. Therefore (1) holds and the "if" part of the theorem follows. Finally, to prove the "only if" part assume $A \not\equiv 1 \pmod 4$ and note that $x^2 - Ay^2 \equiv 0, 1, 2 \pmod 4$, for any integers x and y. This implies that Equation 3.2 has no integral solutions and the lemma follows. □

Lemma 3.2. *Suppose* $Q = [1, 0, -N]$ *or* $[1, N, \frac{1}{4}N(N-1)]$ *and assume* $N \equiv 1 \pmod 4$. *Then the path* γ_Q *contains an elliptic point* τ_e *of order* $e = 2$ *with respect to the action of* $\Gamma^0(N)$.

Proof. By Lemma 3.1 there are coprime integers u and v such that

$$u^2 - Nv^2 = -1.$$

We may also assume $v > 0$. Now if we write $u_1 = 2u$ then

$$u_1^2 - 4Nv^2 = -4.$$

So

$$P = [v, u_1, Nv]$$

defines a primitive form of discriminant $\Delta = -4$ such that its third coefficient is divisible by N. Thus the quadratic imaginary in $\mathcal{H}$ associated to P is an elliptic point τ_e of degree $e = 2$. If we put

$$Q = [1, 0, -N]$$

then it is plain that $\langle P, Q\rangle = 0$. Therefore the elliptic point τ_e of degree $e = 2$ lies in the geodesic γ_Q. Similarly, the form

$$P = \left[2v, 2(u + Nv), Nu + N^2 v - \frac{1}{2}N(N-1)v\right]$$

is primitive of discriminant $\Delta = -4$, and its third coefficient is divisible by N. Thus the point τ_e associated to P is an elliptic point of degree $e = 2$. If we put

$$Q = \left[1, N, \frac{1}{4}N(N-1)\right]$$

it is plain that $\langle P, Q\rangle = 0$. This means that the elliptic point τ_e of degree $e = 2$ lies in the geodesic γ_Q, and the proof is now complete. □

3.2. **Lemma that uses genus theory.** Suppose we have a pair (D, r) that satisfies the Heegner condition, i.e. D is the discriminant of a quadratic order $\mathcal{O}_D$ of conductor f, and $r \in \mathbb{Z}$ is such that

$$r^2 \equiv D \pmod{4N},$$

and $\gcd(f, N) = 1$. Let $\mathcal{Q}_D$ be the set of primitive forms $Q = [A, B, C]$ of discriminant $D = B^2 - 4AC$, and let $\mathcal{Q}_{N,D,r}$ be the set of primitive forms $Q = [A, B, C]$ of discriminant D such that $N \mid C$ and $B \equiv r \pmod{2N}$. Let G_D be the quotient $G_D = \Gamma(1)\backslash\mathcal{Q}_D$ and let $G_{N,D,r}$ be the quotient $G_{N,D,r} = \Gamma^0(N)\backslash\mathcal{Q}_{N,D,r}$. Denote $[Q]_{\Gamma^0(N)}$ (resp. $[Q]_{\Gamma(1)}$) the class of a form Q in $G_{N,D,r}$ (resp. G_D). It is well-known that the natural map $[Q]_{\Gamma^0(N)} \mapsto [Q]_{\Gamma(1)}$ is an isomorphism, as shown by Gross, Kohnen and Zagier [10]. So the set $G_{N,D,r}$ inherits a group structure from the classical composition of classes in G_D due to Gauß [9].

Lemma 3.3. *If $Q = [A, B, C]$ is a primitive form of discriminant $D > 0$ such that $N \mid D$ and $D \mid 4N$, then the image $(\gamma_Q)_{\Gamma_0(N)}$ in $X_0(N)(\mathbb{C})$ of γ_Q is (pointwise) fixed by the reflection w_N^κ, where κ is complex conjugation acting on the set of complex points $X_0(N)(\mathbb{C})$.*

Proof. We need to introduce the following notation. Let the *tip* $\widehat{\gamma}$ of a geodesic $\gamma \subset \mathcal{H}$ be the point

$$\widehat{\gamma} = \frac{x+y}{2} + \left|\frac{x-y}{2}\right| i \in \gamma$$

where $\gamma = \{x, y\}$ and x and y in $\mathbb{R}$. We define the *tip* $\widehat{Q}$ of an indefinite form Q as the positive definite binary quadratic form P such that $\pi_P = \widehat{\gamma_Q}$. If Q is integral we assume $\widehat{Q}$ is primitive. For convenience we divided the proof in three steps as follows.

Step 1. *The image γ in $X_0(N)(\mathbb{C})$ of the path $\gamma_Q \subset \mathcal{H}$ is stable under the action of w_N^κ on $X_0(N)(\mathbb{C})$.* Consider the form $F_N = [N, r, \frac{r^2-D}{4N}]$.[5] On the one hand, it is a well-known fact that for any pair (D, r) satisfying the above mentioned Heegner condition, the diagram

$$\begin{array}{ccc}
[Q]_{\Gamma^0(N)} & \longmapsto & [w_N \circ Q]_{\Gamma^0(N)} \\
G_{N,D,r} & \longrightarrow & G_{N,D,-r} \\
\downarrow & & \downarrow \\
G_D & \longrightarrow & G_D \\
[Q]_{\Gamma(1)} & \longmapsto & [F_N^{-1} Q]_{\Gamma(1)}
\end{array},$$

[5]As remarked in Subsection 1.5.1 of Darmon [8], the class Frob_N in G_D of the form F_N corresponds to the $\mathcal{O}_D$-ideal $\mathfrak{N} = \mathfrak{P}_1 \dots \mathfrak{P}_g$, where $\mathfrak{P}_i$ is the prime ideal of $\mathcal{O}_D$ above the rational prime $p_i \mid N$, for each $i = 1, \dots, g$ (for the general case of N composite).

is commutative. On the other hand, directly from our assumptions $N \mid D$ and $D \mid 4N$, and $D > 0$, we may see that $[F_N^{-1}Q]_{\Gamma(1)} = [Q^\kappa]_{\Gamma(1)}$, where $[A, B, C]^\kappa = [-A, B, -C]$. Therefore

$$[w_N Q]_{\Gamma^0(N)} = [Q^\kappa]_{\Gamma^0(N)}.$$

Hence the involution w_N^κ maps the image γ in $X_0(N)$ of γ_Q onto itself.

Step 2. *The image p^+ in $X_0^+(N)(\mathbb{C})$ of the tip $p = \widehat{\gamma_Q}$ lies in the real locus $X_0^+(N)(\mathbb{R})$.* Suppose we have a pair of integers (Δ, ρ) that satisfies the Heegner condition with $D < 0$, and let $P \in \mathcal{Q}_{N,\Delta,\rho}$. So now $P = [\alpha, \beta, \gamma]$ corresponds to a Heegner point p, assuming of course that $\alpha > 0$. It is well-known that

$$[P^\kappa]_{\Gamma(1)} = [P^{-1}]_{\Gamma(1)},$$

where complex conjugation κ acts on P as $P^\kappa = [\alpha, -\beta, \gamma]$. Thus the condition $w_N^\kappa p = p$ is tantamount to the duplication equation

$$[F_N]_{\Gamma(1)} = [P^2]_{\Gamma(1)},$$

where F_N is the form $F_N = [N, \rho, \frac{\rho^2 - \Delta}{2\alpha}]$. So by the principal genus theorem of Gauß [9], the above equation is equivalent to $\chi(F_N) = 1$, for each (Gauß genus) character

$$\chi : \mathcal{G}_\Delta \longrightarrow \{-1, 1\}.$$

Since N was assumed prime, the value $\chi(F_N)$ of each such character χ may be given in terms of the Kronecker symbol $(\frac{\cdot}{\cdot})$ by the formula

$$\chi(F_N) = \begin{cases} \left(\frac{\Delta_0}{N}\right), & \textit{if } N \nmid \Delta_0 \\ \left(\frac{\Delta_1}{N}\right), & \textit{if } N \mid \Delta_0 \end{cases}$$

for each fundamental discriminant divisor Δ_0 of Δ, where $D_1 \in \mathbb{Z}$ is such that $\Delta = \Delta_0 \Delta_1$ (and $\Delta_1 \equiv 0$ or $1 \pmod 4$ by definition). Clearly to prove that $\chi(F_N) = 1$ for all genus characters χ it suffices to consider only genus characters that arise from *prime* fundamental discriminants $\Delta_0 = -4, -8, 8$ or $(-1)^{\frac{p-1}{2}} p$, where p is and odd prime. Now we specialise the above to the positive definite form $P = \widehat{Q}$ that corresponds to the tip $\widehat{\gamma_Q}$ of γ_Q. In other words, since Q was assumed primitive

$$P = d \left[A, B, \frac{B^2}{2A} - C \right],$$

where $d = \textit{denom}(\frac{B^2}{2A})$. So the discriminant Δ of P may be expressed as $\Delta = d^2 D$, where d is a suitable divisor of $2A$, and D is the discriminant of Q, more explicitly

$$D = \begin{cases} N \textit{ or } 4N, & \textit{if } N \equiv 1 \pmod 4, \\ 4N, & \textit{otherwise.} \end{cases}$$

Recall $D = B^2 - 4AC$ and $N \mid C$. So we have the congruence

$$D \equiv B^2 \pmod{4A}.$$

In particular

$$D \equiv B^2 \pmod{p},$$

for each prime $p \mid 4A$. Since $N \nmid A$, we have $(\frac{D}{p}) = (\frac{N}{p}) = 1$, for each odd prime $p \mid A$. So by the quadratic reciprocity law of Gauß [9] we have

$$\left(\frac{p}{N}\right) = (-1)^{\frac{N-1}{2}\cdot\frac{p-1}{2}},$$

again for each odd prime $p \mid A$. In particular, for each odd prime discriminant divisor $\Delta_0 \mid \Delta$ with $\Delta_0 \neq (-1)^{\frac{N-1}{2}}N$ we have

$$\chi(F_N) = \left(\frac{\Delta_0}{N}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{N}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{N}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{N-1}{2}\cdot\frac{p-1}{2}} = 1.$$

So now it only remains to prove $\chi(F_N) = 1$ for **(1)** $\Delta_0 = (-1)^{\frac{N-1}{2}}N$, and for

$$\Delta_0 = \begin{cases} -4 & \textbf{(2)}, \\ 8 & \textbf{(3)}. \\ -8 & \textbf{(4)}, \end{cases}$$

We address these four cases as follows. Put $\Delta_0 = (-1)^{\frac{N-1}{2}}N$. Since $N \mid \Delta_0$, here we need to show that $(\frac{\Delta_1}{N}) = 1$, where $\Delta_1 \in \mathbb{Z}$ is defined by $\Delta = (-1)^{\frac{N-1}{2}}N\Delta_1$. But this is clear since

$$\chi(F_N) = \left(\frac{\Delta_1}{N}\right) = \left(\frac{-(-1)^{\frac{N-1}{2}}d^2}{N}\right) = (-1)^{\frac{N-1}{2}}(-1)^{\frac{N-1}{2}} = 1,$$

where we assumed by a slight abuse of notation that d^2 includes the factor 4. Thus $\chi(F_N) = 1$ follows for instance **(1)**. Now put $\Delta_0 = -4$. Note $(\frac{\Delta_0}{N}) = (-1)^{\frac{N-1}{2}}$. So it suffices to show that Δ_0 is not a fundamental discriminant divisor of Δ for $N \equiv 3 \pmod{4}$, in other words, that d may not be even. But the congruence $N \equiv 3 \pmod{4}$ implies $B^2 - 4AC = 4N$. Hence B is even, so $AC \equiv 1 \pmod{2}$ and thus A is odd. Therefore $d = denom(\frac{B^2}{2A})$ is odd, and $\chi(F_N) = 1$ follows for instance **(2)**. Suppose $\Delta_0 = 8$. Note

$$\left(\frac{\Delta_0}{N}\right) = \left(\frac{2}{N}\right) = \begin{cases} +1 & \textit{if } N \equiv 1 \textit{ or } 7 \pmod{8}, \\ -1 & \textit{if } N \equiv 3 \textit{ or } 5 \pmod{8}. \end{cases}$$

So let us assume $N \equiv 3$ or $5 \pmod{8}$ and hope for a contradiction. If $B^2 - 4AC = 4N$, then again B is even, so $AC \equiv 1 \pmod{2}$ and thus A is odd, which is clearly not possible. Hence $B^2 - 4AC = N$ and $N \equiv 1 \pmod{4}$. Since $8 \mid d^2$, clearly $4 \mid d$. But B is odd. Therefore A is necessarily even and

$$B^2 \equiv 5 \pmod{8},$$

which is clearly not possible. So $\chi(F_N) = 1$ follows for instance **(3)**. Finally suppose $\Delta_0 = -8$. Note

$$\left(\frac{\Delta_0}{N}\right) = \left(\frac{-2}{N}\right) = \begin{cases} +1 & \textit{if } N \equiv 1 \textit{ or } 3 \pmod 8, \\ -1 & \textit{if } N \equiv 5 \textit{ or } 7 \pmod 8). \end{cases}$$

It is plain that the above argument works here. So $\chi(F_N) = 1$ follows for instance **(4)**.

Step 3. *The map w_N^κ does not fix the image $\gamma^\perp$ in $X^0(N)$ of the geodesic $\{-\frac{B}{2A}, \infty\} \subset \mathcal{H}$.* Since the map w_N^κ is an anti-conformal, involutary automorphism of $X_0(N)$, and the paths γ and $\gamma^\perp$ intersect orthogonally at p, clearly Step1 and Step 2 together imply that w_N^κ acts on the image γ in $X_0(N)$ of $\gamma_Q \subset \mathcal{H}$ as either (1) the identity map, or else (2) the reflection with respect to $\gamma^\perp$. But it is plain that $N \mid B$. Hence

$$w_N^\kappa\left(-\frac{B}{2A}\right) = -\frac{2AN}{B} \in \mathbb{P}^1_{\mathbb{Q}}$$

lies in the $\Gamma^0(N)$-orbit of ∞. So w_N^κ may not fix $\gamma^\perp$, and thus (1) must hold and the proof is now complete. $\square$

3.3. **The construction.** Define the *first half* $\rho^{\frac{1}{2}}_{N,Q,\tau_0}$ of ρ_{N,Q,τ_0} as the restriction of ρ_{N,Q,τ_0} to the interval $[0, \frac{1}{2}l(Q)]$, where $l(Q)$ is the length of ρ_{N,Q,τ_0}. The *antipode* τ_0^{ant} of τ_0 is the end-point $\tau_0^{ant} = \rho_{N,Q,\tau_0}(\frac{1}{2}l(Q))$ of $\rho^{\frac{1}{2}}_{N,Q,\tau_0}$. Finally let γ^+ denote the path in $X_0^+(N)(\mathbb{C})$ induced by a path $\gamma \subset \mathcal{H}$ via the canonical projection map. Theorem 1.1 follows from the following two propositions.

Proposition 3.4. *If $Q_0 = [1, 0, -N]$ and $\tau_0 = \sqrt{-N}$ then $\tau_0^{ant} = \frac{N+\sqrt{-N}}{2}$ and*

$$c_{Q_0}(N) = \{\infty, \tau_0\}^+ * (\rho^{\frac{1}{2}}_{N,Q_0,\tau_0})^+ * \{\tau_0^{ant}, \infty\}^+, \tag{3.3}$$

parametrises the connected component of the real locus $X_0^+(N)(\mathbb{R})$ containing the cusp $i\infty$.

Proof. The proof splits in two cases as follows.

Case A: $N \equiv 1 \pmod 4$. The canonical map $X_0(N)(\mathbb{C}) \longrightarrow X(1)(\mathbb{C})$ is a proper holomorphic map with exactly two branch points b and b' of degree $e = 2$. By Lemma 3.2 we may see that ρ_{Q_0,τ_0} contains one of these branch points, say b. Since complex conjugation

$$\kappa\colon X_0(N)(\mathbb{C}) \longrightarrow X_0(N)(\mathbb{C})$$

maps the underlying set of ρ_{Q_0,τ_0} to itself, we may see that ρ_{Q_0,τ_0} contains the other branch point b'. The same is true for the path ρ_{Q_1,τ_1}, where $\tau_1 = \frac{N+\sqrt{N}}{2}$ and

$$Q_1 = \left[1, N, \frac{1}{4}N(N-1)\right]$$

So ρ_{Q_0,τ_0} and ρ_{Q_1,τ_1} share the branch points b and b'. But by Lemma 3.3 we may see that these regular analytic paths are fixed by the reflection w_N^κ. Therefore, up to orientation and choice of base-point, the paths ρ_{Q,τ_0} and ρ_{Q_1,τ_1} are the same. Now consider that complex conjugation κ fixes the points τ_0 and τ_1 and reverses the orientation of ρ_{Q_0,τ_0}. So τ_1 is the antipode of τ_0 and thus the path $c_{Q_0}(N)$ defined by Equation 3.3 is a closed path contained in the real locus $X_0^+(N)(\mathbb{R})$. (Here we used the fact that κ fixes the geodesic segments $\{i\infty, \sqrt{-N}\}$ and $\{i\infty, \frac{N+\sqrt{-N}}{2}\}$.) Now we claim that $c_{Q_0}(N)$ is smooth. Clearly $c_{Q_0}(N)$ is smooth at τ_0 and τ_1, which are 2-branch points of the canonical covering map

$$X_0(N)(\mathbb{C}) \longrightarrow X_0^+(N)(\mathbb{C}).$$

To prove our claim we only need to verify that no further 2-branch point b of the above covering lies in the path ρ_{Q_0,τ_0}. But this is clear since it is well-known that these 2-branch are Heegner points of discriminant $\Delta = -4N$, or $\Delta = -N$ if $N \equiv 3 \pmod 4$, so Equation 3.2 implies that either $b = \tau_0$ or $b = \tau_1$. So our claim follows and thus it is clear that $c_{Q_0}(N)$ parametrises the connected component of $X_0^+(N)(\mathbb{R})$ containing $i\infty$.

Case B: $N \equiv 3 \pmod 4$. First we claim that all primitive ambiguous forms Q of discriminant $D = 4N$ are $\Gamma^0(N)$-equivalent. Indeed, suppose Q is ambiguous and note $C = [Q]_{\Gamma^0(N)} = [Q^{-1}]_{\Gamma^0(N)}$. Hence

$$[QQ]_{\Gamma^0(N)} = [QQ^{-1}]_{\Gamma^0(N)} = 1,$$

so C has order dividing 2. Since N is an odd prime, genus theory implies that $\#(G_D)$ is odd. Therefore C is the principal class and the claim follows. A consequence of our claim is that the ambiguous forms $Q_0 = [1, 0, -N]$ and $Q_1 = [2, 2N, \frac{1}{2}N(N-1)]$ are $\Gamma^0(N)$-equivalent. This means that the regular paths ρ_{Q_0,τ_0} and ρ_{Q_1,τ_1} are the same, up to orientation and choice of base-point. It is clear that again the point $\tau_1 = \frac{N+\sqrt{-N}}{2}$ is the antipode of the point $\tau_0 = \sqrt{N}$ and that the rest of the proof may be carried out as above. $\square$

Proposition 3.5. *A connected component of $X_0^+(N)(\mathbb{R})$ is parametrised by* ***(A)***

$$c_Q(N) = (\rho_{N,Q,\tau_0}^{\frac{1}{2}})^+$$

if $N \equiv 1 \pmod 4$ and $[Q] \in (G_{N,4N,0} - \{1\}) \cup (G_{N,N,N} - \{1\})$ and by ***(B)***

$$c_Q(N) = (\rho_{N,Q,\tau_0})^+$$

if $N \equiv 3 \pmod 4$ and $[Q] \in G_{N,4N,0} - \{1\}$.

Proof. The proof splits in two cases accordingly.

Case A. By Lemma 3.3 it suffices to prove that $c_Q(N)$ is a smooth, closed, and that it traces out its path only once. By Lemma 3.1 we

may see that the negative Pell equation

$$X^2 - DY^2 = -1$$

has an integral solution, say (u, v). It is plain that the matrix

$$M'_Q = \begin{pmatrix} -u + Bv & 2Cv \\ 2Av & u + Bv \end{pmatrix} \in \Gamma^0(N)$$

is such that $M'_Q \circ [A, B, C] = [-A, B, -C]$. So the canonical image in $X_0^+(N)(\mathbb{C})$ of τ_0 and its antipode τ_0^{ant} are equal. Thus the path $c_Q(N)$ is closed. By an argument similar to the one included in the proof of the above proposition, we may see that ρ_{N,Q,τ_0} may not contain 2-branch points of the canonical covering

$$X_0(N)(\mathbb{C}) \longrightarrow X_0^+(N)(\mathbb{C}).$$

Thus the path $c_Q(N)$ is smooth. It is clear that $c_Q(N)$ traces out its path once and we are done with Case A.
Case B. In this case the associated negative Pell equation has no integral solutions, and thus $[A, B, C] \mapsto [-A, B. -C]$ does not map the underlying set of ρ_{N,Q,τ_0} to itself. It is plain that $c_Q(N) = (\rho_{N,Q,\tau_0})^+$ has the desired properties and the proof is now complete. □

Remark 3.6. Recall that the Fricke involution w_N of $X_0(N)$ may be defined as the automorphism of $X_0(N)$ induced by mapping each isogeny

$$\varphi\colon E \longrightarrow E'$$

with cyclic kernel of order N to its dual

$$\hat{\varphi}\colon E' \longrightarrow E,$$

where the curves E and E' and the isogenies φ and $\hat{\varphi}$ are all defined over $\mathbb{C}$. So a (non-cusp) real point of $X_0^+(N)$ is either such that

$$\varphi^\sigma \cong \varphi \quad \textit{and} \quad E^\sigma \cong E, \tag{3.4}$$

or such that

$$\varphi^\sigma \cong \hat{\varphi} \quad \textit{and} \quad E^\sigma \cong E'. \tag{3.5}$$

Following Ogg [14], the points that satisfy (3.4) come from the real locus of the curve $X_0(N)$ and we call them *old* real points, while the remaining real points are referred to as *new* real points. A connected component of $X_0^+(N)(\mathbb{R})$ that consists only of new points is called a *new* component. Note that the connected component of $X_0^+(N)(\mathbb{R})$ that contains the (only) cusp ∞ is not new, yet it contains new points. All the remaining connected components are new.

4. Coding modulo homology

4.1. **A geometric coding algorithm.** Let *sign*(x) denote the sign of a real number x. We will find convenient to assume the somewhat non-standard convention that *sign*$(0) = 1$, as opposed to the usual *sign*$(0) = 0$.

Definition 4.1. We say an indefinite binary quadratic form $Q = [A, B, C]$ is *reduced*[6] if $B > 0$ and if any of the following two conditions is satisfied.

R1: $2|A + C| < B$
R2: $2(A + C) = -sign(A)B$

From now on let us assume $Q = [A, B, C]$ is an indefinite binary quadratic form with A, B and C in $\mathbb{Z}$. We shall give a geometric interpretation of the concept of reduced indefinite form. Provide the upper half-plane $\mathcal{H}$ with the hyperbolic metric

$$ds = \frac{|d\tau|}{y},$$

where $\tau = x + iy$, with x and y the usual (real-valued) coordinate functions of $\mathbb{C}$. Let $\{\tau_1, \tau_2\}$ denote the (oriented) geodesic that joins a given point $\tau_1 \in \mathcal{H}^*$ to a given point $\tau_2 \in \mathcal{H}^*$. The *geodesic* γ_Q attached to an indefinite form Q is

$$\gamma_Q = \begin{cases} \{\frac{-B-|Q|}{2A}, \frac{-B+|Q|}{2A}\} & \text{if } A \neq 0 \\ \{i\infty, -\frac{C}{B}\} & \text{if } A = 0 \text{ and } B > 0 \\ \{-\frac{C}{B}, i\infty\} & \text{if } A = 0 \text{ and } B < 0 \end{cases}$$

where $|Q|$ denotes the positive square root of $|Q|^2$. We also write $\sqrt{D} = |Q|$, where $D = B^2 - 4AC$. The *intersection number* $I(\gamma_1, \gamma_2)$ of given (oriented) geodesics arcs γ_1 and γ_2 on the upper half-plane $\mathcal{H}^*$ is defined by

$$I(\gamma_1, \gamma_2) = \begin{cases} 1, & \text{if } \#(\gamma_1 \cap \gamma_2) = 1 \text{ and } \{\gamma_1'(P), \gamma_2'(P)\} \text{ has } \textit{positive} \text{ orientation} \\ -1, & \text{if } \#(\gamma_1 \cap \gamma_2) = 1 \text{ and } \{\gamma_1'(P), \gamma_2'(P)\} \text{ has } \textit{negative} \text{ orientation} \\ 0, & \text{otherwise.} \end{cases}$$

where $\gamma'(P)$ denotes the unit tangent vector of a geodesic γ at a point $P \in \gamma$.

Example 4.2. Suppose $Q = [0, 1, 0]$ and $U = [1, 0, -1]$. In fact $\gamma_Q = \{i\infty, 0\}$ and $\gamma_U = \{-1, 1\}$. Clearly γ_Q and γ_U meet at $P = \pi_{[1,0,1]} = i$ (and no other point). In particular $I(\gamma_Q, \gamma_U) = \pm 1$. To determine the sign we note that the tangent vector of γ_Q at P is given by $\gamma_Q'(P) =$

[6]A closely related definition of reduced indefinite form may be found in Choie and Parson's article [4], where $Q = [A, B, C]$ is called reduced if $A > 0$, $C > 0$, and $A + C < B$.

$(0,-1)$, and the tangent vector of γ_U at P is given by $\gamma_U'(P) = (1,0)$. Since the determinant

$$\begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix} > 0$$

we have $I(\gamma_Q, \gamma_U) = 1$.

Put $\sigma = \{\rho_{-1}, \rho_{+1}\}$, where as before $\rho_{\pm 1} = \frac{\pm 1 + \sqrt{-3}}{2}$. Note $\sigma \subset \gamma_U$, where $U = [1, 0, -1]$. To simplify our exposition assume from now on that

$$\boxed{D \textit{ is not a perfect square.}}$$

Now we state without proof some of the results from the author's Cambridge Ph .D. thesis.

Lemma 4.3. *An indefinite form Q is reduced if and only if $I(\gamma_Q, \sigma) = 1$ and $\gamma_Q \cap \mathcal{F}^{int} \neq \emptyset$.*

We call an indefinite form $Q = [A, B, C]$ *nearly reduced* if $3A^2 \leq D$, where $D = B^2 - 4AC$ is the discriminant of Q. To each nearly reduced indefinite form Q we attach the interval $J_Q \subset \mathbb{R}$ defined by

$$J_Q = \begin{cases} \left[t'_{-1}, t'_{+1}\right], & \textit{if } D > 4A^2 \\ \\ \left[t_{-sign(A)}, t'_{-sign(A)}\right], & \textit{if } D < 4A^2 \end{cases}$$

where

$$t_{\pm 1} = \pm\frac{1}{2} + \frac{B + \sqrt{D - 3A^2}}{2A}, \quad \text{and} \quad t'_{\pm 1} = \pm\frac{1}{2} + \frac{B - \sqrt{D - 3A^2}}{2A}.$$

Note that the assumption that Q is nearly reduced guarantees that the end points of the interval J_Q are indeed real.

Lemma 4.4. *Suppose Q is a nearly reduced indefinite form. We have $I(\gamma_{T^t \circ Q}, \sigma) = 1$ if and only if $t \in J_Q$, where $T^t = \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$.*

Corollary 4.5. *If $Q = [A, B, C]$ is an indefinite form such that $\gamma_Q \cap \mathcal{F} \neq \emptyset$, then there is exactly one $t \in \mathbb{Z}$ such that $T^t \circ Q$ is reduced, unless $D < 4A^2$ and either ρ_{-1} or ρ_{+1} lies in γ_Q.*

Lemma 4.6. *Suppose Q is an indefinite form such that either $\rho_{-1} \in \gamma_Q$ or $\rho_{+1} \in \gamma_Q$. Then $\gamma_Q \cap \mathcal{F}^{int} = \emptyset$ if and only if $\gamma_{S \circ Q} \cap \mathcal{F}^{int} \neq \emptyset$.*

Definition 4.7. We say an indefinite form Q is *normalisable* if there is $\delta(Q) \in \mathbb{Z}$ such that $T^{\delta(Q)} \circ Q$ is reduced. Such form $Q^{nrm} = T^{\delta(Q)} \circ Q$ is called its *normalisation.*

Definition 4.8. The *tip* $\widehat{\gamma}$ of a geodesic $\gamma \subset \mathcal{H}$ is the point

$$\widehat{\gamma} = \frac{x+y}{2} + \left|\frac{x-y}{2}\right| i \in \gamma$$

where $\gamma = \{x, y\}$ and x and y in $\mathbb{R}$. We define the *tip* $\widehat{Q}$ of an indefinite form Q as the positive definite binary quadratic form P such that $\pi_P = \widehat{\gamma_Q}$. If Q is integral we assume $\widehat{Q}$ is primitive.

We will find it convenient to consider pointed spaces (γ_Q, τ_0), with $\tau_0 \in \gamma_Q$, e.g. $\tau_0 = \widehat{\gamma_Q}$. By a slight abuse of notation we sometimes write (Q, τ_0) instead of (γ_Q, τ_0).

Algorithm 1: The reduction of Q

Data: (Q, τ_0) with $\tau_0 \gamma_Q$
Result: reduced form Q^{red} equivalent to Q
1 $Q \longleftarrow R_{\tau_0} \circ Q$;
2 **if** $\gamma_Q \cap \mathcal{F}^{int} \neq \emptyset$ **then**
3 $\quad Q \longleftarrow Q^{nrm}$
4 **else**
5 $\quad Q \longleftarrow (S \circ Q)^{nrm}$
6 **end**

Now we prove that Algorithm 1 is correct. First note that the correctness of the classical reduction algorithm of positive definite binary quadratic forms (due to Gauß) implies that after Step 1 the geodesic γ_Q and the (closed) fundamental region $\mathcal{F}$ share at least one point. If also the interior $\mathcal{F}^{int}$ and γ_Q have non-trivial intersection, then Corollary 4.5 implies that the normalisation Q^{nrm} of Q is reduced. However, it may sometimes happen that $\mathcal{F}^{int} \cap \gamma_Q = \emptyset$, which means that γ_Q contains one of the lower vertices of the fundamental region $\mathcal{F}$. But Lemma 4.6 tells us that the transformed form $S \circ Q$ now belongs to the above case, and thus $(S \circ Q)^{nrm}$ is reduced. Therefore Algorithm 1 is correct.

Note that $\Gamma^0(N) = S^{-1}\Gamma_0(N)S$, where $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. By a slight abuse of notation[7] from now on we write

$$X_0(N) = \Gamma^0(N)\backslash\mathcal{H}^*.$$

As before let $Q = [A, B, C]$ be primitive indefinite form with non-square discriminant $D = B^2 - 4AC$. Now define $M_{N,Q} = M_Q^n$, where

$$M_Q = \begin{pmatrix} u - Bv & -2Cv \\ 2Av & u + Bv \end{pmatrix} \in \Gamma(1),$$

and $(u, v) \in \mathbb{Z}$ is a fundamental solution of the ordinary Pell equation

$$X^2 - DX^2 = 1,$$

[7]It is more customary to write $X^0(N) = \Gamma^0(N)\backslash\mathcal{H}^*$. But we want to avoid writing non-standard expressions such as $X_+^0(N)$ (or $X^{0+}(N)$) when considering the Atkin-Lehner quotient defined by the Fricke involution w_N.

and n is the smallest positive integer such that $M_Q^n \in \Gamma_0(N)$. Now pick a base point τ_0 of γ_Q and let $g_{N;Q,\tau_0}$ denote the image of the path $\{\tau_0, M_{N,Q}\tau_0\}$ in the modular curve $X_0(N)$. The construction of the regular path in the proof of Theorem 2.6 carries over to $X_0(N)$ as follows. It is well-known that the elliptic points $\tau_e \in \mathcal{H}$ for the action of $\Gamma^0(N)$ in the upper half plane $\mathcal{H}$ are precisely the ones attached to primitive forms $P = [A, B, C]$ with $N \mid C$ and discriminant $\Delta = -3$, if the degree of the point is $e = 3$ and discriminant $\Delta = -4$, if the degree of the point is $e = 2$. Assume there is an elliptic point τ_e of degree $e = 2$, e.g. $\tau_e = r + \sqrt{-1} \in \mathcal{H}$ with $r \in \mathbb{Z}$ such that

$$r^2 \equiv -1 \pmod N,$$

and that γ_Q contains such elliptic point τ_e. The matrix $S^{\frac{1}{2}}$ in the said construction is to be replaced by $T^r S^{\frac{1}{2}} T^{-r}$, where and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Again let n be the smallest positive integer such that M_Q^n lies in $\Gamma^0(N)$. Further assume that the fundamental unit ϵ of the real quadratic order $\mathcal{O}_D$ has norm $\mathcal{N}(\epsilon) = -1$. The matrix $M_Q^{\frac{1}{2}}$ is to be replaced by $M_{N,Q}^{\frac{1}{2}} = (M_Q^{\frac{1}{2}})^n$, so that $(M_{N,Q}^{\frac{1}{2}})^2 = M_{N,Q}$. Let ρ_{N,Q,τ_0} be the regular analytic path thus obtained and call it the *regular path of level* N attached to Q. This path is unique up to a regular analytic reparametrisation.

Now we need to extend Definition 4.7 to include some indefinite forms Q that arise in Algorithm 2. As before put $\sigma = \{\rho_{-1}, \rho_{+1}\}$. Let $\delta(Q)$ be just as in Definition 4.7, if $D > 4A^2$ and let $\delta(Q)$ be the integer such that the intersection number $I(\gamma_Q + \delta(Q), \sigma) = 1$ (whenever it exists), if $3A^2D < 4A^2$. Assume that Q is N-reduced and that Q is neither close to cusp ∞ nor close to cusp 0. Now put $a = sign(A)$, $d = \delta(Q)$, and define the matrix

$$(4.1) \qquad S_{N,Q} = \begin{cases} T^a S T^{-a}, & \text{if } d = 0, \text{ i.e. } \rho_a \in \gamma_Q & (1) \\ T^{-a\frac{N+1}{2}} S T^{-2a}, & \text{if } \rho_a \in \gamma_Q - a & (2) \\ T^{(d-a)^*} S T^{d-a}, & \text{if } \rho_a \in \gamma_Q + d \text{ and } |d| \neq 1 & (3) \\ T^{d^*} S^{\frac{a}{2}} T^d, & \text{if } i_N \in \gamma_Q & (4) \\ T^{d^*} S T^d, & \text{otherwise,} & (5) \end{cases}$$

where $i_N = i + k$ and $k \in C(N)$ is such that $k^2 \equiv -1 \pmod N$, whenever $N \equiv 1 \pmod 4$, and s^* is the element of $C(N)$ such that $ss^* \equiv 1 \pmod N$, given $s \in \mathbb{Z}$ with $s \not\equiv 0 \pmod N$.

Now we shall consider some examples of N-cycles $(Q)_N = (Q_0, \ldots, Q_{l-1})$ that may help to clarify the above ideas. In the tables below the last column encodes the steps followed while executing the algorithm, using the convention that a number from 1 to 5 indicates one of the five cases of the definition of matrix $S_{N,Q}$, while 0 (resp. ∞) indicates the normalisation step associated to a form close to the cusp 0 (resp. the cusp ∞).

Algorithm 2: The N-cycle of Q

Data: a primitive indefinite binary quadratic form Q

Result: the N-cycle $(Q)_N = (Q_0, Q_1, \dots, Q_{l-1})$ of Q

$Q \longleftarrow Q^{N\text{-}red}$;

$Q_0 \longleftarrow Q$;

$n \longleftarrow 0$;

while $Q \neq Q_n$ *or* $n = 0$ **do**

  if Q_n *is either near cusp* ∞ *or cusp* 0 **then**

    $Q_{n+1} \longleftarrow Q_n^{N\text{-}nrm}$

  else

    $Q_{n+1} \longleftarrow \nu_{Q_n} S_{N,Q_n} \circ Q_n$

  end

  $n \longleftarrow n + 1$;

end

Example 4.9. Suppose $N = 13$. Consider the indefinite form $Q = [-13, 108, -213]$ of discriminant $D = 7^2 \cdot 12$. The N-reduction of $Q^{N\text{-}red} = [11, -70, 98]$ of Q has the following N-cycle.

n	Q_n	M_n	Case
0	$[11, -70, 98]$	$\begin{pmatrix} 3 & -13 \\ 1 & -4 \end{pmatrix}$	5
1	$[-6, 18, 11]$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	0
2	$[-13, -4, 11]$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	5
3	$[2, -26, 11]$	$\begin{pmatrix} 1 & -13 \\ 0 & 1 \end{pmatrix}$	∞
4	$[2, 26, 11]$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	5
5	$[-13, 4, 11]$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	0
6	$[-6, -18, 11]$	$\begin{pmatrix} -4 & -13 \\ 1 & 3 \end{pmatrix}$	5
7	$[11, 70, 98]$	$\begin{pmatrix} -6 & -13 \\ 1 & 2 \end{pmatrix}$	3
8	$[2, -2, -73]$	$\begin{pmatrix} -2 & 13 \\ 1 & -7 \end{pmatrix}$	3
9	$[11, 18, -6]$	$\begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$	0
10	$[11, -18, -6]$	$\begin{pmatrix} -7 & 13 \\ 1 & -2 \end{pmatrix}$	2
11	$[2, 2, -73]$	$\begin{pmatrix} 2 & -13 \\ 1 & -6 \end{pmatrix}$	3

Figure 4.1 depicts the intersection of the geodesics γ_{Q_n}, with the fundamental domain $\mathcal{F}_N$, for $n = 0, 1, 2$ and 3. Similarly, Figure 4.2 depicts the intersection of the geodesics γ_{Q_n}, with the fundamental domain $\mathcal{F}_N$, for $n = 9, 10$ and 11. Note that instance (4) of $S_{N,Q}$ in Equation 4.1 does not take place. This means that the geodesic γ_Q does not contain an elliptic point τ_e of degree $e = 2$.

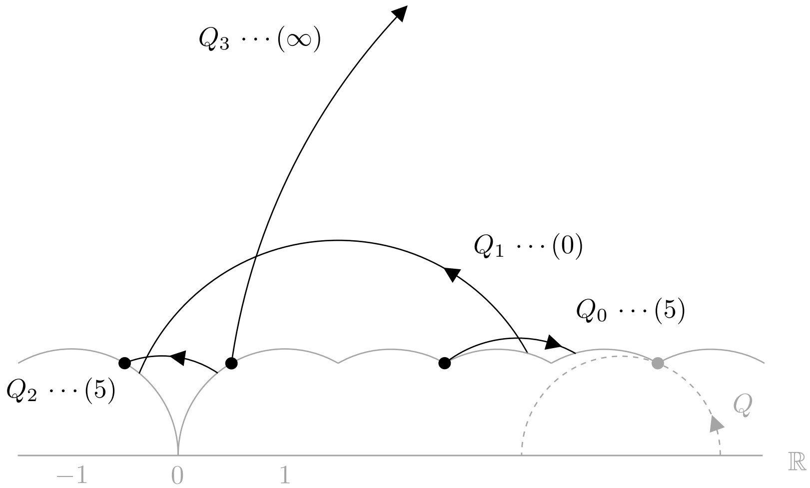

FIGURE 4.1. Beginning of the N-cycle of $Q = [-13, 108, -213]$, with $N = 13$.

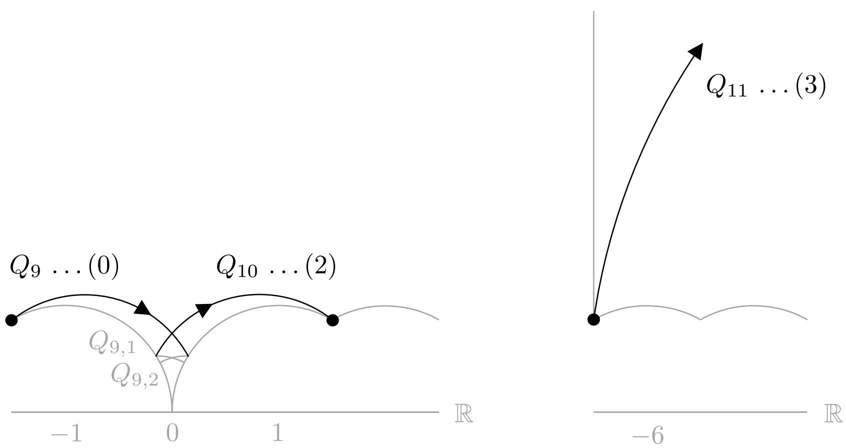

FIGURE 4.2. Near the end of the N-cycle of $Q = [-13, 108, -213]$, with $N = 13$.

Example 4.10. Now suppose $N = 5$ and consider the N-reduced form $Q = [1, -1, -3]$ of discriminant $D = 13$. The N-cycle of Q is as follows.

n	Q_n	M_n	Case
0	$[1, -1, -3]$	$\begin{pmatrix} -1 & 5 \\ -1 & 3 \end{pmatrix}$	4
1	$[3, -16, 17]$	$\begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix}$	∞
2	$[3, 14, 12]$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	3
3	$[1, -10, 12]$	$\begin{pmatrix} 1 & -10 \\ 0 & 1 \end{pmatrix}$	∞
4	$[1, 10, 12]$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$	3
5	$[3, -14, 12]$	$\begin{pmatrix} 1 & -5 \\ 0 & 1 \end{pmatrix}$	∞
6	$[3, 16, 17]$	$\begin{pmatrix} 3 & 5 \\ -1 & -1 \end{pmatrix}$	4
7	$[1, 1, -3]$	$\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$	5
8	$[-1, -5, -3]$	$\begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix}$	∞
9	$[-1, 5, -3]$	$\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$	5

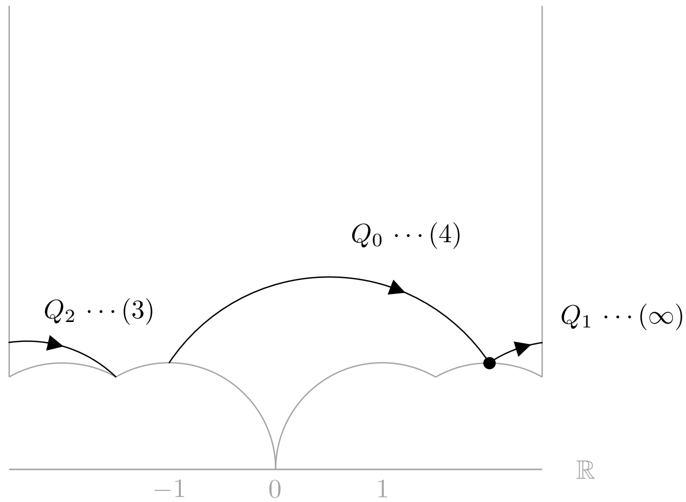

FIGURE 4.3. Beginning of the N-cycle of $Q = [1, -1, -3]$, with $N = 5$.

Figure 4.3 depicts the intersections of the geodesics γ_{Q_n} with the fundamental domain $\mathcal{F}_N$, for $n = 1, 2$, and 3. Note that Q_n falls in case (4), for $n = 0$ and 6. This means that γ_Q contains an elliptic point τ_e of order $e = 2$.

Remark 4.11. It is not hard to see that for each prime $N > 1$, the N-cycle of the indefinite form $Q = [2, 2N, -1]$ is given by

n	Q_n	M_n
0	$[2, 2N, -1]$	$\left(\begin{smallmatrix} 1 & 0 \\ -2N & 1 \end{smallmatrix}\right)$
1	$[2, -2N, -1]$	$\left(\begin{smallmatrix} 1 & -N \\ 0 & 1 \end{smallmatrix}\right)$

Note that the matrices $M_0 = \left(\begin{smallmatrix} 1 & 0 \\ -2N & 1 \end{smallmatrix}\right)$ and $M_0 = \left(\begin{smallmatrix} 1 & -N \\ 0 & 1 \end{smallmatrix}\right)$ are parabolic. So the code $(M_0, M_1, \dots)$ of some indefinite forms Q may consist of parabolic elements only.

Definition 4.12. The N-*code* of Q is the sequence of matrices $(M_0, M_1, \dots)$ defined by $Q_{n+1} = M_n \circ Q_n$, where the matrices M_n come from the computation of the N-cycle $(Q)_N = (Q_0, Q_1, \dots Q_l)$ of Q using Algorithm 2.

4.2. **Conversion of each component into M-symbols.** As before let Q be an indefinite binary quadratic form of discriminant $D = B^2 - 4AC > 0$. Recall we assumed D is non-square.

Definition 4.13. Write $s = Z(\gamma)$. The M-*cycle* $\mu(\gamma)$ associated to a N-reduced geodesic $\gamma = \gamma_Q$ is the sum

$$\mu(\gamma) = \{i\infty, \widehat{\gamma}\} + \{\widehat{\gamma}, i + s\} + \left\{i + s, \widehat{\gamma'}\right\} + \left\{\widehat{\gamma'}, i\infty\right\},$$

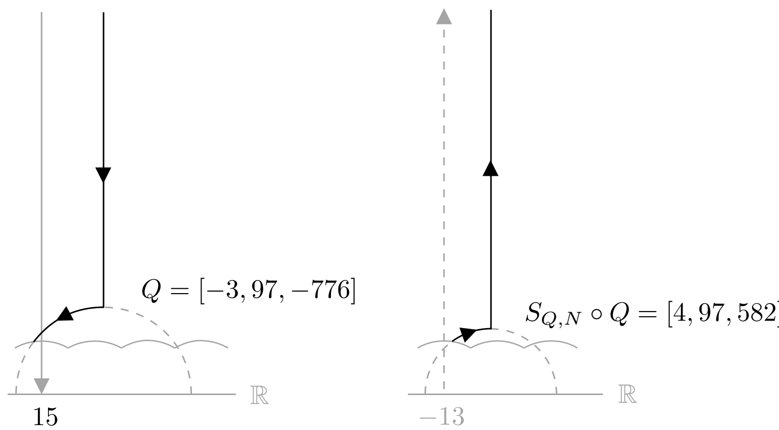

FIGURE 4.4. Example of path $\mu(\gamma_Q)$ associated to Q for $N = 97$.

where $\gamma' = \gamma_{Q'}$, $Q' = (T^s S^{\frac{a}{2}} T^{-s}) \circ Q$ with $a = sign(A)$, if $s = s'$ and $T^{-s}\gamma_Q$ contains i, and

$$\mu(\gamma) = \{i\infty, \widehat{\gamma}\} + \{\widehat{\gamma}, P\} + \left\{M_s P, \widehat{M_s\gamma}\right\} + \left\{\widehat{M_s\gamma}, i\infty\right\}$$

where $P = \gamma_Q \cap \{s-1, s+1\}$, otherwise.

Example 4.14. Suppose $N = 97$ and let $\gamma = \gamma_Q$ with $Q = [-3, 97, -776]$. We may see γ is N-reduced, with $Z(\gamma) = 15$. Note $r \neq r'$. This means we are in the second case. We have $M_s \circ Q = [4, 97, 582]$. Thus

$$\mu(\gamma) = \{i\infty, \widehat{\gamma}\} + \{\widehat{\gamma}, P\} + \left\{M_s P, \widehat{M_s\gamma}\right\} + \left\{\widehat{M_s\gamma}, i\infty\right\},$$

where $\widehat{Q} = \frac{97+\sqrt{-97}}{2\cdot 3}$, $P = \frac{208+8\sqrt{-3}}{2\cdot 7}$, $M_s P = \frac{180+8\sqrt{-3}}{2\cdot 7}$, and $\widehat{M_s \circ Q} = \frac{-97+\sqrt{-97}}{2\cdot 4}$, as shown in Figure 4.4.

Example 4.15. Suppose $N = 97$ and consider the form $Q = [-9, -338, -4171]$. We have $s = s' = -22$, and $T^{-s} \circ Q = [-9, 8, 9]$ is such that $A + C = 0$. This means we are in first case. Moreover,

$$S^{-\frac{1}{2}} \circ [-9, 8, 9] = [-4, -18, 4]$$
$$T^{-22} \circ [-4, -18, 4] = [-4, -194, -2328].$$

Note $sign(A) = -1$. So $M_s \circ Q = [-4, -194, -2328]$, and therefore

$$\mu(\gamma) = \{i\infty, \widehat{\gamma}\} + \{\widehat{\gamma}, i+s\} + \left\{i+s, \widehat{\gamma'}\right\} + \left\{\widehat{\gamma'}, i\infty\right\},$$

where $\widehat{\gamma} = \frac{-338+\sqrt{-4\cdot 97}}{2\cdot 9}$ and $\widehat{\gamma'} = \frac{-97+\sqrt{-97}}{2\cdot 2}$, as shown in Figure 4.5.

Lemma 4.16. *Assume the notation of Definition 4.13. In the first case the image of $\mu(\gamma)$ on $X_0(N)$ is homologous to 0, while in the second case the image of $\mu(\gamma)$ on $X_0(N)$ is homologous to the M-symbol $(s : 1)$.*

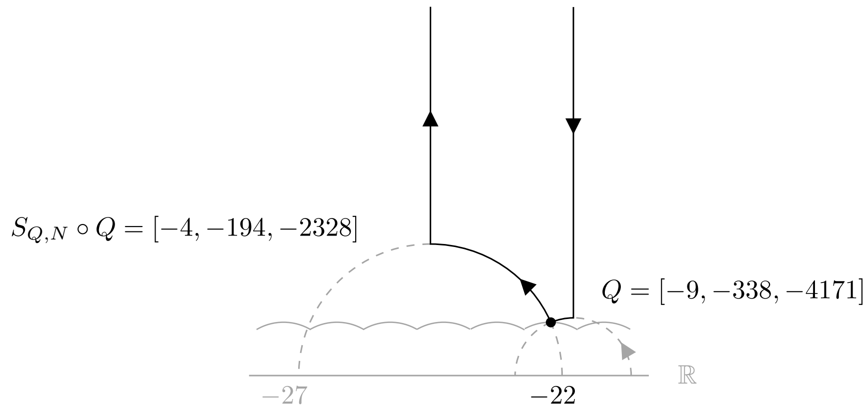

FIGURE 4.5. Example of path $\mu(\gamma_Q)$ associated to Q for $N = 97$.

Proof. The first part is obvious. So we assume in particular that $s \neq s'$. Since we are working with $\Gamma^0(N)$ orbits, the bijection of Proposition 2.2.2 of Cremona [6] identifies the M-symbol $(s : 1)$ with $\{i\infty, s\}$. Write $C_{s,r} = \{s - r, s + r\}$, with r real . For each $r \geq 1$ the geodesic $C_{s,r}$ intersects the path $\{i\infty, \widehat{\gamma}\} + \{\widehat{\gamma}, P\}$ at exactly one point, say A_r, and $C_{s,r}$ also intersects the path $\{i\infty, i + s\}$ at exactly one point, say B_r. Similarly, for each each $r \geq 1$ the geodesic $C_{s,r}$ intersects the path $\{M_s P, \widehat{M_s\gamma}\} + \{\widehat{M_s\gamma}, i\infty\}$ at exactly one point, say A'_r, and $C_{s,r}$ also intersects the path $\{i+s', i\infty\}$ at exactly one point, say B'_r, where s' is the (unique) solution to the congruence $s's \equiv -1 \pmod N$ such that $|s| \leq \frac{N-1}{2}$. Consider the one parameter families of geodesic arcs

$$\mathcal{G} = \{\{A_r, B_r\} \colon r \geq 1\} \quad \text{and} \quad \mathcal{G}' = \{\{A'_r, B'_r\} \colon r \geq 1\}.$$

Using M_s we may glue (in the sense of topology) the image of $\mathcal{G}$ on $X_0(N)$ with the image of $\mathcal{G}'$ on $X_0(N)$. Denote $\mathcal{I}$ the one parameter family of geodesic arcs on $X_0(N)$ thus obtained. Since both, $\mathcal{G}$ and $\mathcal{G}'$ are contained in the closure $\mathcal{F}_N^{clo}$ of the fundamental domain $\mathcal{F}_N$, we see that we may "push" the image of the path $\mu(\gamma)$ on $X_0(N)$ along $\mathcal{I}$ to obtain an homotopy to the image of

$$\{i\infty, i + s\} + \{i + s', i\infty\}$$

on $X_0(N)$. Obviously this path is equal to the image of $\{i\infty, s\}$ on $X_0(N)$, and the lemma follows. $\square$

Theorem 4.17. *The homology class $[\rho_{N,Q,\tau_0}]$ in $H_1(X_0(N), \mathbb{Z})$ of the regular path ρ_{N,Q,τ_0} may be expressed in terms of M-symbols as*

$$[\rho_{N,Q,\tau_0}] = \sum_{n=0}^{l-1} (r_n : 1)$$

where

$$r_n = \begin{cases} -(M_n)_{2,2}, & \textit{if } Tr(M_n) > 2, \\ 0, & \textit{otherwise} \end{cases}$$

and $M_0, \ldots, M_{l-1}$ *is the* N*-code associated to the* N*-cycle* $(Q)_N = (Q_0, \ldots, Q_{l-1})$ *of* Q*, and* $M_{i,j}$ *denotes the* i, j*-entry of matrix* M*.*

Proof. The theorem follows from the definition of Algorithm 2 and Lemma 4.16. □

Now we work out some examples where the above theorem is applied. Let Ω_E denote the least positive real period of the Néron differential ω_E of E. Now for each form Q as in either Proposition 3.4 or Proposition 3.5 define the period

$$\Omega_{E,Q} = \frac{1}{2\pi i} \int_{c_Q(N)} f(\tau) d\tau,$$

where $f(\tau)$ denotes the newform attached to E,[8] and define the integer $\alpha_{E,Q}$ by the equation

$$\Omega_{E,Q} = \alpha_{E,Q} \Omega_E.$$

In the following examples we compute $\alpha_{E,Q}$ using Theorem 4.17, and the rapidly convergent series of Cremona [7].

Example 4.18. Suppose $N = 37$ and write $Q = [1, 0, -37]$. The first half of the N-cycle and the corresponding N-code of ρ_{N,Q,τ_0} is given by

n	K_n	M_n
0	$(1, 0, -37)$	$T^6 \frac{1}{2} S^{\frac{1}{2}} T^{-6} *$
1	$(3, -37, 111)$	$\left(\begin{smallmatrix} -16 & 111 \\ 1 & -7 \end{smallmatrix}\right)$

Where the symbol $*$ is placed next to the non-hyperbolic matrix. (See Figure 4.6.) In particular $[c_Q(N)] = (7 : 1)$. So the period of $c_Q(N)$, with respect to the holomorphic differential ω_f attached the newform $f_E(\tau)$ is $\omega_1 = 2.9934586462319\ldots$, which is of course the real period associated to the Néron differential of elliptic curve **37A1**. Therefore $\alpha_{E,Q} = 1$.

Example 4.19. Again suppose $N = 37$. The set $S_{N,4N,0}$ consists only of the class of the form $Q = [3, 74, 444]$. So $[Q]$ gives rise to a connected

[8]Note that whenever the path γ_Q contains an elliptic point τ_e of degree $e = 2$, the integral

$$r_{N,Q}(f) = \int_{\tau_0}^{M_Q \tau_0} f(\tau) d\tau$$

in p. 500 of the article of Gross, Kohnen and Zagier [10] (defined there for arbitrary positive even weights) vanishes, whereas the closely related integral $\Omega_{E,Q}$ usually does not.

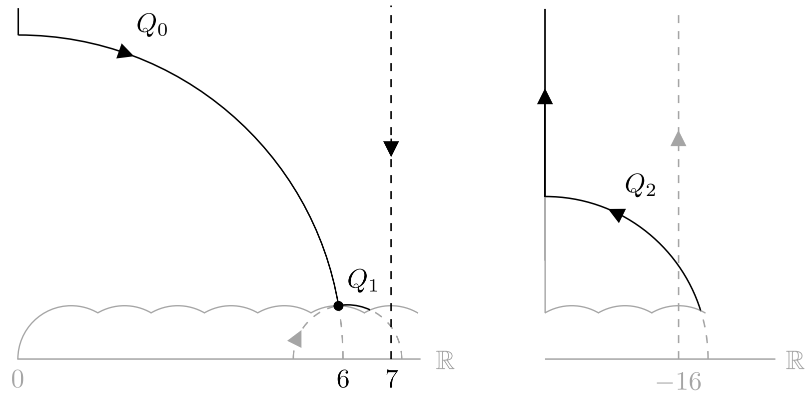

FIGURE 4.6. A connected component $c_Q(N)$ for $N = 37$.

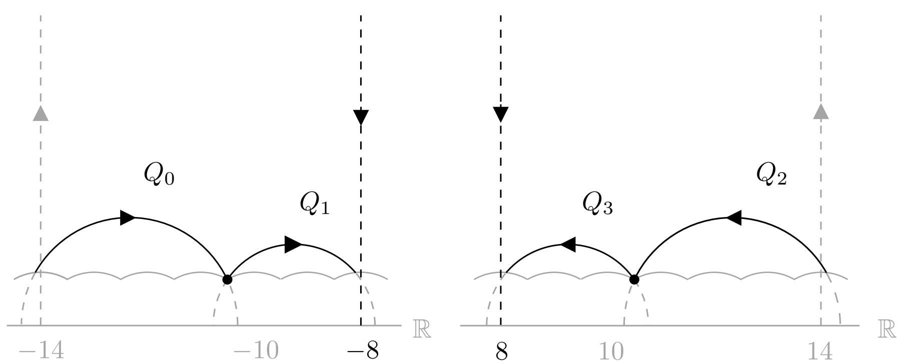

FIGURE 4.7. A connected component of $X_0^+(N)$ for $N = 37$.

component of $X_0^+(N)_{\mathbb{R}}$ other than the one that contains the only cusp of $X_0^+(N)$. The corresponding N-cycle of Q is as follows.

n	Q_n	M_n
0	$[3, 74, 444]$	$\left(\begin{smallmatrix} -11 & -111 \\ 1 & 10 \end{smallmatrix}\right)$
1	$[4, 74, 333]$	$\left(\begin{smallmatrix} 14 & 111 \\ 1 & 8 \end{smallmatrix}\right)$
2	$[-3, 74, -444]$	$\left(\begin{smallmatrix} 11 & -111 \\ 1 & -10 \end{smallmatrix}\right)$
3	$[-4, 74, -333]$	$\left(\begin{smallmatrix} -14 & 111 \\ 1 & -8 \end{smallmatrix}\right)$

See Figure 4.7. Thus

$$2[c_Q(N)] = (-8:1) + (8:1).$$

Similarly we may found that again $\alpha_{E,Q} = 1$.

Example 4.20. Suppose $N = 79$. The only element $[Q] \in \mathcal{S}_{N,4N,0}$ is represented by the form $Q = [7, 316, 3555]$. Recall curve $X_0^+(N)$ is isomorphic to the elliptic curve E known as **79A1**. The corresponding

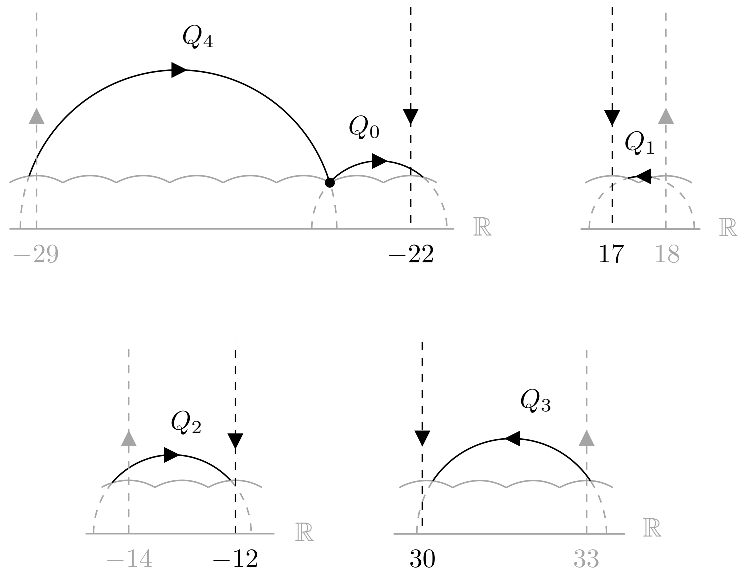

FIGURE 4.8. A connected component of $X_0^+(N)_{\mathbb{R}}$ for $N = 79$.

N-cycle of Q may be described as follows.

n	Q_n	M_n
0	$[7, 316, 3555]$	$\begin{pmatrix} 18 & 395 \\ 1 & 22 \end{pmatrix}$
1	$[-9, 316, -2765]$	$\begin{pmatrix} -14 & 237 \\ 1 & -17 \end{pmatrix}$
2	$[6, 158, 1027]$	$\begin{pmatrix} 33 & 395 \\ 1 & 12 \end{pmatrix}$
3	$[-5, 316, -4977]$	$\begin{pmatrix} -29 & 869 \\ 1 & -30 \end{pmatrix}$
4	$[3, 158, 2054]$	$\begin{pmatrix} -24 & -553 \\ 1 & 23 \end{pmatrix}$

See Figure 4.8. We have

$$[c_Q(N)] = (-22 : 1) + (17 : 1) + (-12 : 1) + (30 : 1)$$

Similarly we may obtain $\alpha_{E,Q} = 1$.

Example 4.21. Suppose $N = 163$ and put $Q = [1, 0, -163]$. We have the following table.

n	Q_n	M_n
0	$[1, 0, -163]$	$\begin{pmatrix} 25 & -326 \\ 1 & -13 \end{pmatrix}$
1	$[6, -326, 4401]$	$\begin{pmatrix} -45 & 1304 \\ 1 & -29 \end{pmatrix}$
2	$[-7, -652, -15159]$	$\begin{pmatrix} 17 & 815 \\ 1 & 48 \end{pmatrix}$
3	$[9, -326, 2934]$	$\begin{pmatrix} 60 & -1141 \\ 1 & -19 \end{pmatrix}$
4	$[-11, 1304, -38631]$	$\begin{pmatrix} 59 & -3423 \\ 1 & -58 \end{pmatrix} *$
5	$[-3, 326, -8802]$	$\begin{pmatrix} -75 & 3749 \\ 1 & -50 \end{pmatrix}$

Where again the symbol $*$ is placed next to the non-hyperbolic matrix.

$$[c_Q(N)] = (13) + (29) + (-48) + (19) + (50)$$

Now consider the elliptic curve E known as **163A1** in Cremona's Tables [5]. Since the sign s of the functional equation of E is $s = -1$, then we have a modular parametrisation

$$\varphi^+ \colon X_0^+(N) \longrightarrow E.$$

Let f be the newform attached to E. (This is the first example of an elliptic curve of rank 1 and prime conductor that is a proper quotient of $J_0^+(N)$.) Similarly we may find that the period of the connected component $c_Q(N)$ with respect to ω_f coincides with the real period $\omega_1 = 5.518073071224596\ldots$ of the Néron differential of E. Thus again $\alpha_{E,Q} = 1$.

References

1. M. Akbas, *The normalizer of modular subgroups*, University of Southampton Ph.D. thesis (1989).
2. M. Akbas and D. Singerman, *Symmetries of modular surfaces*, Discrete groups and geometry (Birmingham, 1991), London Math. Soc. Lecture Note Ser., vol. 173, Cambridge Univ. Press, Cambridge, 1992, pp. 1–9.
3. A. F. Beardon, *The geometry of discrete groups*, Graduate Texts in Mathematics, vol. 91, Springer-Verlag, New York, 1995, Corrected reprint of the 1983 original.
4. Y. Choie and L. A. Parson, *Rational period functions and indefinite binary quadratic forms. II*, Illinois J. Math. **35** (1991), no. 3, 374–400.
5. J. E. Cremona, *Elliptic curves of conductor* $\leq 20,000$, http://www.maths.nott.ac.uk/personal/jec/ftp/data/.
6. ———, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.
7. ———, *Computing periods of cusp forms and modular elliptic curves.*, Exp. Math. **6** (1997), no. 2, 97–107.
8. H. Darmon, *Heegner points, Heegner cycles, and congruences*, Elliptic curves and related topics, CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., Providence, RI, 1994, pp. 45–59. MR **95i:**11064
9. C. F. Gauß *Disquisitiones arithmeticae*, Translated into English by Arthur A. Clarke, S. J, Yale University Press, New Haven, Conn., 1966.
10. B. H. Gross, W. Kohnen, and D. B. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), no. 1–4, 497–562.
11. S. Katok, *Coding of closed geodesics after Gauss and Morse*, Geom. Dedicata **63** (1996), no. 2, 123–145.
12. A. M. Legendre, *Théorie des Nombres*, third ed., vol. I, Chez Firmin Didot Frères, Libraires, Rue Jacob, N° 24, Paris, 1830.
13. Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.
14. A. P. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 277–307.
15. P. C. Sarnak, *Prime geodesic theorems*, Stanford Ph.D. thesis (1980).
16. Goro Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.
17. A. Weil, *Number theory. An approach through history from Hammurapi to Legendre*, Birkhäuser Boston, Inc., Boston, Mass., 1984.

E-mail address: `ccastanobernard@gmail.com`
URL: `http://sarva.no-ip.info/ccb/index.html`